Communication barriers in the decision-making process: System Language and System Thinking

Stef Schinagl
VU University Amsterdam and Noordbeek
stef@noordbeek.com

Ronald Paans
VU University Amsterdam and Noordbeek
ronald.paans@noordbeek.com

Abstract

A major problem in the decision-making process is poor communication regarding threats and risks between information security experts and decision makers. By their nature, experts have a strong interest in operational details and limited insight into the purpose of the organization as they may not fully understand the mission and business. They are overusing System Language and System Thinking. This means they will fail making themselves fully understood by the decision makers, who are therefore not able to make carefully considered risk-based decisions.

This paper describes the theory behind the underlying communication problem between information security experts and decision makers and the use of System Language and System Thinking. We questioned 63 participants, observed and analyzed their opinions, and discussed the results. This has led to Lessons Learned for developing a curriculum on Information Security and Privacy Protection (IS&PP) and defining areas for further research.

1. Introduction

The importance of information security and privacy protection (IS&PP) is growing and it is fast becoming a vital aspect of the quality of our everyday life. In today's business world, information is one of the most important assets [4, 15, 29]. Information has become the life blood of the company and seems even necessary to gain competitive advantage [5, 7, 21, 29]. The big challenge today is to ensure that a company's (digital) information is protected against possible risks which can arise against this information [28].

To protect information assets clear IS&PP governance should be implemented as the overall manner in which information security is deployed to mitigate risks [32]. Therefore, decision makers need to rely on there IS&PP experts [3]. But as long as IS&PP is handled as a technical matter instead of a business issue [5, 14, 32, 34], and as long as experts persist in overusing System Language and System Thinking [24], the communication and knowledge-sharing problem will continue to occur.

1.1. Background

Corporate Governance dictates that executives realizes the mission of an organization, considering the real risks. Therefore, decision makers must understand and assess the risks and their possible impact on the business processes. All entities face uncertainty and the challenge for decision makers is to determine how much uncertainty can be accepted [8]. To make such risk-based decisions in the field of IS&PP, information security needs to be incorporated in organizational structures. This means not only involving technical experts at an operational level but also involving senior management and executives i.e. the decision makers [32, 34].

1.2. Decision makers

In general, managing risks is undeniably a responsibility of the decision makers [8, 16, 21, 28]. Risk management supports decision makers, allowing their responsibility of protecting the valuable information assets of their enterprises [20].

But often they lack the knowledge and expertise regarding risk management, as they tend to be generalists [3, 21, 30]. Risks are (1) not identified, (2) not understood, (3) ignored or (4) have become lost between those with knowledge and the decision maker [23, 24, 25].

In the specific case of IS&PP, this abyss yawns even wider [23, 30]. Firstly, as most organizations become more dependent on IT and information, executives and senior management still tend to ignore the importance of appropriate measures for IS&PP to protect these valuable assets [23, 25]. Decision makers focus on the functionality of the information systems and how to make money with data, while security is a non-functional. They are reluctantly forced to spend attention, money and manpower on this non-functional factor, although it feels it does not contribute to their profit directly.

URI: http://hdl.handle.net/10125/41902
ISBN: 978-0-9981331-0-2

Secondly, although some studies show that attention for information security in board rooms is increasing [34], we still see occurring low levels of for instance, presence of CIO in board levels or lack of IS&PP expertise among board members [3, 21]. Due to lack of knowledge and expertise, decision makers feel that they are not sufficiently equipped to discuss IS&PP topics, let alone make well-deliberate risk-based decisions about it [15, 23, 25].

But one cannot expect decision makers to master all domains of risk [18]. Therefore, they must solicit advice from there skilled IS&PP experts who make the real risks visible. Boards may come to rely quite heavily on the expertise and knowledge of IS&PP experts to assist them with there IS&PP governance duty. However, the ultimate accountability and decision making remains theirs alone [3, 15].

1.3. IS&PP Experts

IS&PP experts are not always assisting the decision makers properly. Although extensive and thorough literature can be found on accepted IS&PP risk management approaches [4, 8, 10-13, 17, 20], it seems that the real risks to the organization performing its mission are often not understood.

Possible causes of this failure can be found in literature, such as that these generally accepted approaches demand very detailed knowledge about the IT security domain and the actual company environment [4, 26]. Although the approaches provide detailed information about potential threats, vulnerabilities, and countermeasures, they lack the required organizational context and guidelines.

This lack leads to experts focusing on technological and procedural aspects rather than on mission and business aspects, resulting in poor risk-based information for the decision makers [8].

In general, many experts work at a level that is too detailed, fail to identify the real risks for the mission, and are therefore unable to communicate these risks to the executives and managers in an understandable language [5]. '*No decision takes place in vacuo: there is always a context*' [23]. Without this organizational knowledge and expertise, it is almost impossible to consider the complex web of risks for IT security and risks for the organization's mission [4]. It seems that decision makers and IS&PP experts live in different worlds.

2. Research Method

In designing the research approach the 'Design Science Research Methodology for Information Systems', is used as presented by Vaishnavi and Kuechler in 2013 [31]. This paper combines the research models of some other authors, such as March and Smith (1995), Owen (1997), Peffers (2008) and Gregor and Hevner (2013). Design Science Research (DSR) starts with a clear problem definition and iteratively follows a cycle of phases. Because partial completion or failure in following phases leads back to the awareness of the problem [31], DSR relies heavily on a clear problem definition. Therefore, the research presented in this paper focuses mainly on describing, motivating and substantiating the problem of ineffective communication and insufficient knowledge-sharing between the IS&PP experts and the decision makers. Following phases are part of a larger PhD research program and are only briefly referred to in this paper.

2.1. Awareness of a problem phase:

According to Vaishnavi, awareness of an interesting problem may come from multiple sources. This study defines a communication and knowledge-sharing problem due to different worlds and people failing to speak each other's language [9, 24]. The disjunction between different worlds has been analyzed and modeled to determine the communication problem.

The theory of the three disjunctive worlds is presented and discussed in different setting such as workshops and lectures. On the basis of the modeled theory, a questionnaire is developed to measure the opinion about the potential communication problem and the recognition and appreciation of the theory. Both a group of 36 student participants and 27 project professionals are questioned. Analyses of the results are performed and questions are clustered to understand how the participants deal with the problem described.

We presented our draft conclusions to the academic review group at our University. The academic review group consist of two IT audit professors, two executives, two risk managers and three students associated with our University. These debates have led to a proposal for adapting the curriculum and initiating further research.

2.2. Following Phases: Related Research

As educators we focus on providing our experts with a broader and more in-depth insight and experience on who they need to communicate with and in which way. The expert is the link-pin providing meaningful analysis and advice to the decision makers. Communication and knowledge-sharing must focus upon the 'Value at Risk' determined from the mission of the organization [24, 25]. This approach allows the experts and their messages to support the decision makers and to be useful in

making carefully considered decisions. During the lectures the opinions of the students are measured. These surveys do not only focus on the theory presented but also on the deductive methods. This leads to insights which can be used for continuously renewing and modernizing the education methods in the field of IS&PP.

Since there is a natural barrier, merely recognizing the problem or teaching about it is not the only solution [25]. The IS&PP expert and the decision maker should be jointly supported by a model that helps to identify real business risks, which is understandable to the World of Mission and the Real World. The authors of this paper have developed an Information Assurance Cube, which provides a structured method for the IT risk expert performing a risk analysis bridging the gap between expert and decision maker [24, 25].

3. Theoretical model: The Different Worlds

We have analyzed a model to visualize and further outline the natural boundaries of the different worlds. Dutch researcher Wouter Hart explains the problem that an increasing number of organizations believe that rules and procedures contribute to more control [9]. Hart defines a 'Real World' where interaction exists between customers and employees versus a world of systems, rules and procedures, specifically the System World. The theory suggests that organizations sometimes believe that 'optimizing' the System World through more information systems, procedures, policies, frameworks etc. is beneficial to achieve the goals of the Real World. However, the consequence is that more distance is created between the worlds, inevitably leading to failure to achieve the mission and vision of an organization.

This model is applied to the communication and knowledge-sharing problem described in this article. More substance is given to the abstract conceptual model developed by Hart. In order to give a brief explanation, we physically locate decision makers in the World of Mission or Real World and the experts in the System World.

3.1. 'World' of Mission: Purpose

The executives are expected to define the strategy of the organization and to guide middle and lower management in motivating the staff to reach the business goals. It could be said that they set the tone at the top. The executives deal with the mission and communicate with their peers, such as their Board of Supervisors, regulatory authorities, accountants, executives of other organizations and government agencies, and their division directors [9].

These executives often only have an implicit connection to the Real World and hardly have any direct connection to the System World. They are concerned about the continuity of their organization, laws and parliamentary decisions affecting the business positions, their own career, etc. Although the executives understand risk within the World of Mission, they are not always fully aware of the threats and risks arising from the two underlying worlds potentially impacting the mission. They must assume that lower-level managers have taken appropriate measures, but cannot be sure about it.

3.2. Real World

The Real World is where the organization meets the customers, achieves business goals and earns money. This world is governed by strict objectives such as market position, customer base, and profit. Therefore, senior management in the Real World has clear responsibilities. They are heavily involved with their own concerns about retaining customers and staff, managing staff, solving personal problems among the staff, fulfilling their profitability obligations, ensuring customer satisfaction, etc. [9].

The Real World needs support from systems and procedures to create a manageable and controlled environment. The System World realizes a major part of this support.

3.3. System World

The System World is where the procedures, forms, information systems, databases, websites, standards, etc. are developed, maintained and enforced. Often there is some friction between the Real World, striving for flexibility and profitability, and the System World, always looking for perfection and assurance [9].

In the System World, we often find highly specialized experts around the systems who are involved in the procedures. They should support the business in achieving its goals. Wouter Hart notes that the focus of controlling organizations is too much oriented towards a System World perspective [9]. According to Hart, it is a myth that more procedures, systems and rules lead to a more controllable organization, let alone greater success. Because of this system-oriented approach, we lose track of the goals from the Real World, the World of Mission, and their underlying purpose.

3.4. Evaluation of the interaction between the worlds

There are factors that influence a risk-based decision, for example environmental context [4, 23]. But

there are also factors regarding the failing communication problem which are directly related to the expert [6]. Experts tend to use technical jargon, not relating the insights to the manager's situation or starting with details before an overview is given [6]. Experts tend to overestimate familiarity with technical terms at the limits between everyday language and specialized jargon. In consequence, they overestimate how well non-experts understand what they communicate [6]. Also experts sometimes find it difficult to articulate their knowledge or rephrase their insights in a way that non-experts can relate to. An insight seems self-evident to them, whereas others actually find it difficult to grasp [6]. These examples are referred to as System Language.

Every person handles real and perceived risks in their own way . There is no common approach to decision-making, due to personal attitudes and specific circumstances. Business managers perceive these risk experts as acting from within the System World since they primarily verify the procedures and the use of the systems and lack the environmental context [4, 26]. The attitude of many of these experts in the System World is 'rather be safe than sorry', where managers in the Business World have a more risk prone attitude [23]. In short, 'people hear what they want to hear'. This means that recommendations from the experts are ignored when they clash with the beliefs and expectations of the decision maker in the Real World and World of Mission. An example of System Thinking is when communicating their analysis results, experts do not tailor their insights to the knowledge of the decision maker, as they assume that the target group already has a similar understanding of an issue [6].

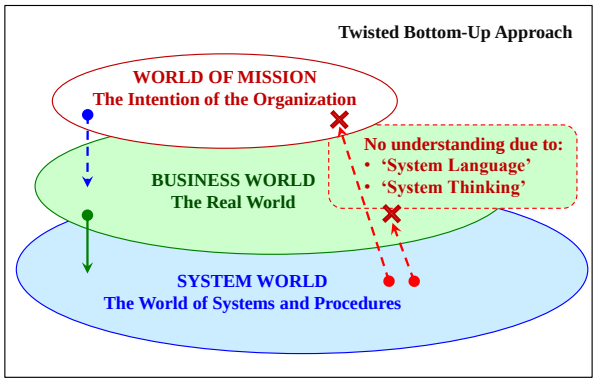

Figure 1. Twisted Organizations

The problem is that the activities of these groups are limited to their own view [9, 26, 27] the worlds are in fact disjunctive. There is a natural barrier between the worlds as each of the worlds has its own qualities and interests which are vastly different. In theory, IS&PP experts' risk-based information should be organized from a top-down vision. With regard to risk management, this means listening to the 'tone at the top', i.e. focusing on the risks to the mission and the business objectives and speaking a business language [20, 24, 25]. A risk-based approach could help people understand how information security affects their organization's missions and business objectives, establishing which assets are important to the organization and how they are at risk [1].

In practice, many experts lack experience in using such a top-down approach. Their assessments are based upon the work methods and standards commonly used within the System World. This leads to 'System Thinking' and 'System Language'. In such a case, a twisted organization is created, often without an integral approach to risk management. The World of Mission and Business World will only understand and accept a risk if they recognize the risk as affecting their mission and business processes [5]. Many of the risks signaled from within the System World fail in this respect [26].

4. Measurements and Results: Problem Definition

The theory of the three disjunctive worlds has been presented and discussed in different setting such as workshops and lectures. On the basis of the theory presented, a questionnaire is developed to measure the opinion of the participants about potential communication problem and their recognition and appreciation of the theory. We analyze the results in the following paragraphs and discuss the outcome in a separate chapter.

4.1. Population of Students

In total 36 students participated in the research. The average age of the participants is 27 years. While the course is strongly focused on the IT-audit field, we see a growing diversity among the students. While in the past more than 80% of the students worked as an active IT auditor, we now observe that the major part of the group (47%) work as IT-consultant in the broad domain of information security with specializations in fields such as cybersecurity, data analytics and risk management. There is still a significant group of active IT auditors (39%) within the population.

4.2. Population of Project Professionals

The 36 students are relatively novice participants with an average of almost four years work experience. Their work experience is for 71% IT related. They are now active in an IT-related job and are recognized to be

IT experts within the System World. Due to their professional background, their opinion and statements about the experts and decision makers may easily be biased.

Therefore, the observations are expanded by involving a second group, in this case consisting of 27 experienced project professionals because they also have a role in the decision-making process [22]. They are active in governmental agencies and have an average of 15,1 years work experience, of which 63% is IT-related. This high amount of IT-related work experience was not anticipated in advance, as a more general business profile was expected. Since they are project managers, they are also acting from a System World perspective.

4.3. Research topics

The answers are rated on a five-point scale where (1) equals 'do not agree at all' and (5) equals 'fully agree'. In addition to the quantitative approach, there is also the option to substantiate the given answer. This enables more qualitative results. The two groups are coded as St = Students (experts within the System World) and Pr = Project Professionals. The total group is Tt = Total Participants.

The questionnaire included 32 questions, often formulated in the form of statements to measure the amount of agreement. In this paper 15 of these questions are discussed. We have performed an analysis of the results and clustered the questions to understand how the participants think about the theory presented. The questions Qx are clustered to cover the following topics:

Topic 1: Do the participants recognize the theory about the different worlds? (Q: 1, 2, 3, 4, 13, 14, 15)

Topic 2: What is the opinion of the participants about experts versus decision makers within the decision-making process? (Q: 5, 6, 7, 8, 9)

Topic 3: Do the participants recognize the use of System Language and System Thinking? (Q:10, 11, 12)

4.4. Recognition of the worlds

The questionnaire starts with:

Q1*: Do you support the theory about the three disjunctive worlds?*

Q2*: Do you recognize this theory within your own work environment?*

The participants express confirmation with Q1 about the three disjunctive worlds. The results are 'Q1 agree' = 73% and 'Q1 fully agree' = 18%. So 91% is positive about the model. For Q2 about recognition within their own environment, the results are 'Q2 agree' = 81% and 'Q2 fully agree' = 14%. This is in total 95%. The remaining participants were neutral, none of them invalidated the model or disagreed with the questions.

Q3*: The three worlds are in fact disjunctive, which leads to limitations in the interaction and communication due to different interests.*

Statement Q3 is not supported by the majority of respondents. The result is 'Tt Q3 disagree or do not agree at all' = 59%. For the questions Q1 and Q2 there was no notable difference in the answers between the groups Students and Project Professionals. However, for Q3 we notice 'St Q3 disagree' = 63%, of which 'St Q3 fully disagree' = 11%, versus 'Pr Q3 disagree' = 36%, of which only one participant fully disagreed. A possible explanation for the difference could be found in variables age and work experience, as there is a positive correlation between these variables and Q3. It might be that experiencing the disjunctive worlds during a longer time, the project professionals could have accepted this phenomenon as unavoidable. Hence 64% of them does not reject the statement Q3.

The students reason from a theoretical perspective and assume that the worlds should not be disjunctive, as some of their comments state that relationships between the worlds are vital. Two of these comments are: '*You need interaction in all three worlds to achieve your ultimate goal*' and '*The wider the gap, the more chaos there will be*'.

Q4*: We experience that the System World dominates with an overkill in rules and procedures;*

Q13*: A growing System World is necessary because this leads to more efficiency, control, etc.;*

Q15*: The System World should always facilitate the Real World.*

The majority of all participants agree with Q4 about domination, with 'Tt Q4 agree' = 60%. A very small group of only 10% disagree with nobody fully disagreeing. Also a majority of the participants confirm Q15 that the System World should facilitate the Real World, with 'Tt Q15 agree or fully agree' = 80%. This may suggest that the participants feel uncomfortable with rules and procedures as this might hamper achieving goals.

The results for Q13 about the growing System World show a different view. Especially, only a small group of the students believes that an ever-expanding System World is not efficient, with 'St Q13 disagree or do not agree at all' = 16%. This is in contrast with the vision of the theoretical model that shows that more rules can be stressful for organizations in achieving their mission. In addition, the results of the project professionals also do not show a dominant opinion, with 'Pr Q13 agree'= 42% and 'Pr Q13 disagree' =44%.

Q14*: We believe in a makeable world, because with more rules and procedures we have more control.*

One of the participants fully agrees and 41% agrees. They indicate that due to the technical developments, an increasing number of rules and procedures are required and that modern techniques may improve the manageability of these environments. Other participants indicated the rules provide certainty and trust and are sometimes necessary for performing their day-to-day job. Very few mention that these rules and procedures should be proportionate to the risks, nor that too many rules create a risk for the achievement of an organization's mission. The participants' belief in a makeable world is contrary to the vision of Wouter Hart [9].

4.5. Opinions about Manager and Expert

***Q5**: Executive and senior management is responsible for decisions regarding IS&PP.*

Although the manager is a generalist with often limited knowledge of IS&PP, he or she is always responsible for decision making. This responsibility is recognized by the majority of the participant, with 'Tt Q5 agree' = 57% and 'Tt Q5 fully agree' = 13%. Only one participant completely disagrees. Comments are similar for both proponents (> neutral) and opponents (<neutral). Proponents of Q5 comment that the manager should not make a decision if he or she has insufficient knowledge about the topic. To quote two comments: '*A manager should acquire sufficient knowledge to make decisions*' and '*A manager who makes decisions without sufficient knowledge is an unprofessional manager*'.

***Q6**: Executives acknowledge the importance of IS&PP.*

None of the participants completely disagrees with Q5. On average, 46% agrees with Q6. The comments explain that most executives acknowledge IS&PP, However, the underlying question is whether the executive actually acts on risks related to IS&PP or gives higher priority to directly business-related issues and Key Performance Indicators (KPIs). There is a substantial discrepancy between the groups Pr and St as 'Pr Q6 agree' = 70% and 'St Q6 agree' = 31%. The majority of the students are neutral 'St Q6 neutral = 55%. The difference between Pr and St is due to doubts by the students whether executives really understand what IS&PP means, while the project professionals think more from a management perspective.

***Q7**: The decision makers have a sufficient amount of knowledge about IS&PP to make well deliberate risk-based decisions.*

Acknowledging IS&PP is one thing but having sufficient knowledge and understanding for IS&PP is another. Most participants disagree that the decision maker has sufficient knowledge about IS&PP to make effective risk-based decisions, with 'Tt Q7 disagree' = 59%, without a difference between the two groups.

***Q8**: A decision maker must have substantive knowledge about IS&PP.*

If a decision maker knows the details of IS&PP, he or she does not need experts. The participants do not have a clear opinion about Q8 whether the decision maker really should possess such knowledge. There is a slight preference to disagree, with 'Tt Q8 disagree' = 37%. The minor difference between the two groups is 'St Q8 fully agree' = 0% versus 'Pr Q8 fully agree' = 11%. Only one student fully disagrees with Q8, see Table 1.

Table 1. Q8 Cross tabulation

Count (%)	Students	Project Professionals
Do not agree at all	1 (3%)	0 (0%)
Disagree	14 (39%)	9 (33%)
Neutral	14 (39%)	7 (26%)
Agree	7 (19%)	8 (30%)
Fully Agree	0 (0%)	3 (11%)
Total count	36	27

***Q9**: The decision maker needs experts to support the decision-making process.*

A large group of the participants believe that the decision maker needs experts in making a carefully considered decision, with 'Tt Q9 > agree'= 90% whereof 'Tt Q9 fully agree' = 27%. It would seem that the participants think they are important to the decision makers.

4.6. System Language and System Thinking

In the following questions the communication and knowledge-sharing problems caused by the overuse of the System Language and System Thinking is discussed.

***Q10**: Use of technical terms and operational details from the expert leads to poor communication and risk-based information between expert and decision maker (message is not understood).*

Even though the misuse of the correct language is a form of critique on the performance of the expert, most of the participants that are experts agree on the statement that risk-information sharing and message is not understood due to System Language, with 'Tt Q10 agree' = 64% and 'Tt fully agree' = 6%. Quite some students still disagree as 'St Q10 disagree' = 22%, where none of the project professionals disagree ('Pr Q10 disagree' = 0%). There is one participant (Pr #15) that fully disagrees in the group project professionals with Q10, i.e. the only team manager (see Table 2).

Table 2. Q10 Cross tabulation			
Count (%)	Students	Project Professionals	Team Manager
Do not agree at all	0 (0%)	0 (0%)	1 (2%)
Disagree	8 (22%)	0 (0%)	0 (0%)
Neutral	5 (14%)	5 (19%)	0 (0%)
Agree	21 (58%)	19 (73%)	0 (0%)
Fully Agree	2 (6%)	2 (8%)	0 (0%)
Total count	36	26	1

The opponents to Q10 explain that if the expert uses System Language too often, the experts are not professional. Some students believe that sometimes the business lacks an interest in the detailed environment of the experts. A more positive explanation about overuse of System Language says that we should not underestimate the intelligence of the business and that the business sometimes understands System Language very well, but maybe just have other priorities that the experts does not understand.

Q12*: Experts do not tailor their insights to the decision makers' environments leading to no action from the decision makers due to valueless information (message is not understood due to System Language).*

For Q12, we see the same pattern as in the results for the System Language in Q10. The minor difference is that some project professionals now disagree as 'Pr Q12 disagree' = 12%. Again the team manager is the only one to fully disagree to Q12. A striking illustration of one of the qualitative comments from the participants is that the use of System Language and System Thinking is logical because the IS&PP expert still reasons from a System World perspective. This student also mentions that limited attention is spent on this specific problem in practice and from a training and educational perspective.

Q11*: Experts do not understand the decision-making environment.*

It is not clear why the participants show different answers on Q11, stating that the experts do not understand the decision-making environment. While they agree on Q10 and Q12, a large part of them disagrees to Q11 (42,9%). It could be that the question is formulated too negative or is too confronting.

4.7. Influence of variables

Differences between the Student group and Project Professional group is not the only valuable approach that could contribute to underpinning the results. By considering additional factors in the data analysis with variables as Age, Work experience and IT-related work experience in relation to the questions, more profound understanding behind the data is sought. Because scale data (age, work experience and It-related work experience) are correlated with ordinal (Qx) data a Spearman Rank Correlation is used.

Most of the questions show weak positive correlations, lower than 0.2 on all of the scale variables. This means that the higher the age or the more work experience, the more the participants agree on the questions. The more specific the scale variables go from age, work experience to IT-related work experience the lower the correlations get. For the questions Q1, Q2 and Q4 we could find a positive significant correlation within all scale variables. For all variables, the correlations for Q13 and Q14 are weak negative and not significant.

Based on the theoretical model the assumption was that the longer you are active in the System World the more you recognize the underlying theory presented in this paper. Because we expected that for experts this would be most recognizable we focused on the correlation of IT-related work experience with the different questions. The positive significant correlations are:

Table 3. IT Related Work Experience			
Correlations:	Question		
Spearman's rho	Q1	Q2	Q4
Correlation Coefficient	.252*	.272*	.321*
Sig. (2-tailed)	.048	.031	.011
N (count)	62	63	62
* Correlation is significant at the 0.05 level (2-tailed).			

These positive significant correlations demonstrate that the more IT-related work experience the participants have the more:

- The participants support the theory about the three Worlds (Q1);
- The theory about the worlds is recognized in practice (Q2);
- The participants experience that the System World dominates and that there is an overkill in rules and procedures (Q4.)

There are two weak negative correlations with the variable IT-related work experience. The only negative weak and not significant correlations Q13 = -0.069 and Q14= -0.117 explain that that the more IT-related work experience the less we agree on:

- That a growing System World is necessary because this leads to more efficiency control (Q13);
- That with more rules and procedures, we have more control, 'the makeable world' (Q14).

Although the correlation is weak, it does contribute to the validity of the results. Q13 and Q14 are verification questions, so it is expected that contrary results can be found.

5. Discussion Results: Future research and limitations

The comments on the results by topic are as follows.

5.1. Topic 1: Recognition of the worlds

The participants strongly recognize the existing communication and knowledge-sharing problems, but they still attach a high value to rules and procedures and believe that these contribute to controlling our businesses. This statement is especially true among the student group. However, the challenge is to understand that even though these rules, methods and procedures are helpful and sometimes necessary, when communicating our message, we have to understand the business interests and needs. We believe that when this definition of the problem is broadly recognized, there are a variety of approaches to define solutions, e.g. with the aid of education [2]. The reason that an educational solution can contribute in solving the problem is that the correlation results show that the less experienced the less the problem is recognized. Paying attention in an early stage of the career can add value to the performance in the future. The main benefit would not only be convincing the students about the theory, but stimulating the dialogue regarding the experiences and opinions, which may contribute to interesting insights about this topic.

5.2. Topic 2: Opinion about managers and experts

The participants are convinced decision makers recognize IS&PP as an important factor for the business. This is in line with the trend found in the studied literature. First senior management seemed to ignore IS&PP [23, 30]. However, now more IT knowledge can be found in board rooms, although still not with satisfying numbers [3, 15, 21]. This is mainly confirmed by the project professionals. The students do not have a clear opinion, as the majority is neutral. This could be explained due to less direct experience and interaction with decision makers.

The ultimate accountability and decision making remains the responsibility of the decision makers alone [3, 8]. Still a major part of the population finds that decision makers lack sufficient knowledge to make well-deliberate decisions. But it should be observed that sufficient knowledge among decision makers is a relative concept in the context of questioning IS&PP experts or project professionals with dominant IT-related work experience.

The participants do not have a clear opinion whether the decision makers should actually have detailed knowledge about IS&PP. This still is an area for further research. For instance, during the 9th IFIP/WISE9 conference in May 2015, a panel discussion on 'Building National Cybersecurity Work Forces' for IFIP Working Group 11.8 was held. The objective of the panel was to discuss the level of expertise of IS&PP professionals within companies and the need for further education methods, techniques, materials, etc. The audience also discussed investing in more attention in education or training the decision makers, such as managers, directors, politicians, etc. No consensus was reached about a possible solution to this question, nor was a clear vision reached during this interesting discussion. Also roles and responsibilities of board members and senior executives with regard to information security have received only limited attention in recent academic literature [15].

5.3. Topic 3: System Thinking and System Language (limitation)

It was remarkable to find a team manager within the project professional group. We first wanted to exclude this participant from the dataset as it might unintentional influence the results. However, during the discussion of the results it turned out to be an eye opener.

In Q10 the participants (experts) recognize the overuse of System Language. The message is not understood and eventually leads to no action from the decision makers. But the team manager was the only participant to not agree at all. In other words, System Language may be used as it is understood by decision makers, but still decision makers can have other priorities whereby no follow-up is given to findings. The focus can then be placed to explore the problem behind System Thinking but also 'Q12 do not agree at all' is answered only by the team manager. Since he or she is the only one with a more business related function, the assumption cannot be relied on but it is clear that further research is recommended.

It is necessary to collect more qualitative data from potential participants with a strong business background as it was not expected that the project professionals had such an large amount of IT-related work experience. Lack of business results is a limitation to this research and is strongly recommended as future research. Additional results will contribute to develop a targeted solution for the described communication and knowledge-

sharing problem about the interaction between the experts and the decision makers from a business perspective, as already some initiatives show [15].

Experts confess and recognize the overuse of System Language and System Thinking. The results for this research remain valid for focusing and finding solutions for the experts' point of view.

6. Insight in changing the curriculum

After our presentation to the academic review group at the University, this group decided to adapt the curriculum for the next year by paying more attention to communication for risk managers and IT-auditors. The students must become professionals who are able to judge the threats, risks and effectiveness of the existing system measures from a mission and business perspective [33].

The current 2½-year curriculum consists of an initial six months of Administrative Organization and Internal Control, similar to the education of accountants. The second year covers IT Governance, IT Risk Management & Compliance, Application Architecture, Software Development, Project Management, etc., in accordance with Cobit 5.0 [11, 28], and training advisory skills. The third year deals with the technical and organizational infrastructure of IT [13], i.e. platforms, networks, ITIL processes, etc.

It has been decided to extend the second year with six workshops, each taking a full working day, training the students in the World of Mission and the Business World [33]. During the workshops they should not act as IS&PP expert, but as an executive who lives in the hectic and dynamic world of the mission and business. Students will be trained to handle a large number of important and urgent issues. The trainers will be senior managers of multinational corporations and governmental departments, with much experience in providing structure and solutions at boardroom level. Some trainers are Lean Six Sigma Black Belts, who are skilled to eliminate the eight kinds of waste, i.e. defects, overproduction, waiting, non-utilized talent, transportation, inventory, motion and extra-processing (abbreviated as 'downtime') [27]. They attempt to reduce the 'System Thinking' as described in this paper, and to stimulate the students moving from using 'System Language' to formulating in business and mission language by setting the right priorities for their messages to the World of Mission and the Business World. So the experts will have a higher added value for senior management and executives.

7. Conclusion

Communication and knowledge sharing between experts and decision makers must operate from the 'Value at Risk' determined from the mission of the organization [24, 25]. Through such prioritization of the risks and relevant mitigating measures, the expert can formulate a message that is understood and appreciated by executives and senior management [12]. This approach allows the experts and their messages to support the decision makers and to be useful in making carefully considered decisions.

8. References

[1] Alberts, C. J., Dorofee, A., Managing information security risks: the OCTAVE approach, Addison-Wesley Longman Publishing Co, 2002.

[2] Blakley, B., McDermott, E., et al., 'Information Security is Information Risk Management', New Security Paradigms Workshop, 2001.

[3] Coertze, J., Von Solms, R., 'The Board and IT Governance: A Replicative Study', African Journal of Business Management, 7(36), 2013, 3358.

[4] Ekelhart, A., Fenz, S., Neubauer, T., 'Aurum: A Framework for Information Security Risk Management', Hawaii International Conference on System Sciences (HICSS), 2009.

[5] Entrust, Information Security Management ISG Framework, An Essential Element of Corporate Governance, April 2004.

[6] Eppler, M., 'Knowledge communication problems between experts and decision makers: an overview and classification', The Electronic Journal of Knowledge Management, 5(3), 2007, pp. 291-300.

[7] Ezingeard, J. N., McFadzean, E., Birchall, D., 'Mastering the art of corroboration: A conceptual analysis of information assurance and corporate strategy alignment', Journal of Enterprise Information Management, 20(1), 2007, pp. 96-118.

[8] Flaherty, J.J., Maki, T., 'Enterprise Risk Management Integrated Framework: Executive Summary', Committee of Sponsoring Organizations of the Treadway Commission (COSO), September 2004.

[9] Hart, W., 'Verdraaide Organisaties: Terug naar de Bedoeling', ('Twisted Organizations, Back to the Mission') (in Dutch) Vakmedianet Deventer, ISBN 978-90-23-20573-5, 2nd ed., 2012.

[10] IRAM, 'Information Risk Assessment Methodology (IRAM)', Information Security Forum (ISF), 2011.

[11] ISACA, 'A Business Framework for the Governance and Management of Enterprise IT, Cobit 5.0', Information System Audit and Control Association, 2012.

[12] ISF, 'The 2011 Standard of Good Practice for Information Security', Information Security Forum, June 2011.

[13] ISO/IEC 27001:2013, 'Information Security Management System, Requirements', BSI, 1 October 2013.

[14] Johnston, A.C., Hale, R., 'Improved security through information security governance', Communications of the ACM, 52(1), 2009, pp. 126-129.

[15] McFadzean, E., Ezingeard, J. N., Birchall, D., 'Perception of risk and the strategic impact of existing IT on information security strategy at board level'. Online Information Review, 31:5, 2007, pp. 622-660.

[16] NIST Special Publication SP800-30, 'Risk Management Guide for Information Technology Systems', Revision 1, September 2012.

[17] NIST Special Publication SP800-37, 'Guide for Applying the Risk Management Framework to federal Information Systems, A Security Life Cycle Approach', Revision 1, February 2010.

[18] NIST Special Publication SP800-39, 'Managing Information Security Risk', March 2011.

[19] NIST Special Publication SP800-53, 'Security and Privacy Controls for Federal Information Systems and Organizations', Revision 4, April 2013.

[20] Peltier, T.R., 'Information Security Risk Analysis', Taylor & Francis Group, ISBN 0-8493-3346-6, 2de ed., 2005.

[21] Posthumus, S., Von Solms, R., King, M., 'The board and IT governance: The what, who and how', South African Journal of Business Management, 41(3), 2010, pp. 23-32.

[22] Prpic, J., 'Project Risk Management Incorporating Knight, Ellsberg & Kahneman', Proceedings of the 49th Annual Hawaii International Conference on System Sciences, Kauai, Hawaii, January 2016.

[23] Riaback, A., 'Managerial Decision Making Under Risk and Uncertainty', IAENG International Journal of Computer Science (IJCS) 32:4, 2012.

[24] Schinagl, S., Paans, R., 'A 2020 vision on educating experts for risk-informed decision making for information security', Submitted to HICSS'49, 2016.

[25] Schinagl, S., Paans, R., 'The Revival of Ancient Information Security Models, Insight in Risk and Selection Measures', Proceedings of HICSS'49, http://www.computer.org, Kauai, Hawaii, January 2016.

[26] Siponen, M., Willison, R., 'Information Security Management Standards: Problems and Solutions', Information & Management, 46, June 2009, pp. 267-270.

[27] Skalle, H., Hahn, B., 'Applying Lean, Six Sigma, BPM, and SOA to Drive Business Results', IBM Redguides REDP-4447-01, 18 April 2013.

[28] Von Solms, S.H., Von Solms, R. Information security governance, Springer US, 2009.

[29] Von Solms, R., Thomson, K.L., 'Maninjwa, M., Information security governance control through comprehensive policy architectures', Information Security South Africa (ISSA), IEEE, 2011, pp. 1-6.

[30] Straub, D.W., Welke, R.J., 'Coping with System Risk: Security Planning Models for Management Decision-Making', MIS Quarterly 22:4, 1998.

[31] Vaishnavi, V., Keuchler, B., 'Design Science Research in Information Systems', 8th International Conference on Design Science Research in Information Systems and Technology, Helsinki, Finland, 2013.

[32] Veiga, A. D., Eloff, J. H., 'An information security governance framework', Information Systems Management, 24(4), 2007, pp. 361-372.

[33] VU University Amsterdam, Post Graduate School, 'IT Audit, Compliance & Advisory Faculty, Curriculum 2015-2016'.

[34] Williams, P., Information security governance, Information security technical report, 6(3), 2001, pp. 60-70.